UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Seizure of
(Briefly describe the property to be seized)

Binance Holdings Ltd cryptocurrency exchange account wallet 0x9510c00aaac3561ef75f7b111edfcba1278333b6 for Binance User ID 130389609

Case No. 1:23mJ43

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Middle District of North Carolina is subject to forfeiture to the United States of America under 18 U.S.C. § 981(a)(1)(A) and (C) & 18 USC 982(a) *describe the property)*:

All cryptocurrency, virtual currency, funds, monies, and other things of value stored in or accessible at Binance Holdings Ltd cryptocurrency exchange account wallet 0x9510c00aaac3561ef75f7b111edfcba1278333b6 for Binance User ID 130389609

The application is based on these facts:

See attached Affidavit.

☑ Continued on the attached sheet.

Applicant's signature

Steven S. Robinson, Special Agent, USSS
Printed name and title

In accordance with Rule 4.1(b)(2)(A), the Applicant attested under oath to the contents of this Application, which was submitted to me by reliable elecronic means, on this 26 day of January, 2023, at 4:48 a.m./p.m.

Date: 1/26/2023

Judge's signature

City and state: Winston-Salem, North Carolina

Joi Elizabeth Peake, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA.

IN THE MATTER OF THE SEIZURE OF All cryptocurrency, virtual currency, funds, monies, and other things of value stored in or accessible at the following Binance Holdings Ltd cryptocurrency exchange accounts wallet 0x9510c00aaac3561ef75f7b111edfcba1278333b6 for Binance User ID 130389609 wallet 0xf85db42fc79b153eac3725f0382fadaa34bae40a for Binance User ID 100785154	Case No. 1:23 MJ 43

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEIZURE WARRANTS

I, United States Secret Service Special Agent Steven S. Robinson, hereby depose and state as follows:

INTRODUCTION

1. I submit this affidavit in support of combined criminal and civil seizure warrants for all cryptocurrency, virtual currency, funds, monies, and other things of value stored in or accessible at the following Binance Holdings Ltd d.b.a. "Binance" (which owns and operates the Binance cryptocurrency exchange) accounts (collectively, the "SUBJECT ACCOUNTS"):

a. Binance User ID 130389609, suspected conspirator Mehmet Sultanoglu, wallet address 0x9510c00aaac3561ef75f7b111edfcba1278333b6 (SUBJECT ACCOUNT #1); and

b. Binance User ID 100785154, suspected conspirator Sun Zhenzhe, wallet address 0xf85db42fc79b153eac3725f0382fadaa34bae40a (SUBJECT ACCOUNT #2).

2. Based on my training and experience and the facts set forth in this Affidavit, there is probable cause to believe that unknown subjects have violated Title 18, United States Code,

Sections 1343 and 1349 (wire fraud and conspiracy to commit wire fraud) and laundered the proceeds of that activity in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) and 1956(h) (money laundering and conspiracy to commit money laundering). There is also probable cause to believe that the SUBJECT ACCOUNTS received the proceeds of the wire fraud scheme described below and are therefore subject to seizure and forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and Title 28, United States Code, Section 2461(c). Moreover, as indicated below, there is also probable cause to believe the SUBJECT ACCOUNTS are involved in money laundering transactions and are therefore subject to seizure and forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 982(a)(1). Accordingly, I request that the Court authorize the attached warrant for seizure of the assets described herein.

3. This Affidavit is intended to show only that there is sufficient probable cause for the requested forfeiture seizure warrants described more fully below and does not set forth all of my knowledge about this matter. The information contained herein comes from my personal knowledge; information conveyed by law enforcement officers and cryptocurrency exchange representatives; and publicly available information.

AFFIANT BACKGROUND AND EXPERTISE

4. I am a Special Agent (SA) with the United States Secret Service (USSS). I have been employed with the USSS as a Special Agent since February 19, 2019. I have completed extensive training at both the Criminal Investigator Training Program at the Federal Law Enforcement Training Center, Glynco, GA and the Special Agent Training Course at the USSS training facility located in Beltsville, MD. Prior to my employment with the USSS, I was a Special Agent with the Diplomatic Security Service of the U.S. Department of State for three years. During my time with the USSS, I have completed over 400 hours of training in cyber and computer-related

investigations, and have completed an additional 50 hours of training specific to cryptocurrency and cryptocurrency investigations. As a USSS Special Agent, I have participated in the seizure of cryptocurrency from wallets on exchanges on four occasions.

FORFEITURE AUTHORITY AND PROCEDURE

5. *Wire fraud forfeiture*: Title 18, United States Code, Section 981(a)(1)(C) provides that "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable" to the violation of an enumerated statute constituting a specified unlawful activity "is subject to forfeiture to the United States." Specified unlawful activities are detailed therein, as well as at Title 18, United States Code, Sections 1956(c)(7) and 1961(1), which enumerates Title 18, United States Code, Section 1343 as a specified unlawful activity. This section provides both civil forfeiture authority and criminal forfeiture authority by virtue of Title 28, United States Code, Section 2461(c).

6. *Money laundering forfeiture*: Title 18, United States Code, Section 981(a)(1)(A) provides for the civil forfeiture of any property, real or personal, that is involved in a transaction or attempted transaction in violation of Title 18, United States Code, Sections 1956, 1957, or 1960. Title 18, United States Code, Section 982(a)(1) provides for the criminal forfeiture of any property, real or personal, that is involved in a transaction or attempted transaction in violation Title 18, United States Code, Sections 1956, 1957, or 1960.

7. *Seizure warrant authority*: Title 18, United States Code, Sections 981(b)(2) and (3) provide that seizures executed for purposes of civil forfeiture shall be made pursuant to a warrant issued in the same manner as provided for a criminal search warrant under Federal Rule of Criminal Procedure 41. Moreover, seizure warrants may be issued in any district in which a forfeiture action may be filed and may be executed in any district in which the property is found.

Pursuant to Title 28, United States Code, Section 1355, a civil forfeiture action may be brought in any district in which any of the acts or omissions giving rise to the forfeiture occurred, including in this case, as detailed below, the Middle District of North Carolina. Accordingly, the Court may issue a civil forfeiture warrant in this district to be executed on property found in another judicial district.

8. Title 28, United States Code, Section 2461(c) provides that the procedures (including seizure warrants) in Title 21, United States Code, Section 853 control criminal forfeiture. Section 853(f) of the same title provides that the government may request a warrant for the seizure of property for forfeiture in the same manner as it may seek a search warrant. Title 18, United States Code, Section 982(b)(1) also provides that seizures for criminal forfeiture shall be made pursuant to a warrant issued in the same manner as provided for a criminal search warrant under the Federal Rules of Criminal Procedure, and cross-references Title 21, United States Code, Section 853. This warrant seeks seizure authority under both the criminal and civil forfeiture statutes.

9. Title 21, United States Code Section 853(f) provides that a court may issue a criminal seizure warrant when it "determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a[] [protective] order under [21 U.S.C. § 853(e)] may not be sufficient to assure the availability of the property for forfeiture." As set forth further below, there is a substantial risk that the funds in the SUBJECT ACCOUNTS will be withdrawn, moved, dissipated, or otherwise become unavailable for forfeiture unless seized. I therefore submit that a protective order under 21 U.S.C. § 853(e) would not be sufficient to assure that the funds in the SUBJECT ACCOUNTS will remain available for forfeiture.

BACKGROUND OF CRYPTOCURRENCY

10. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

11. *Cryptocurrency and Blockchain Generally*: Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Tether, USD Coin, and DAI. Each unit of cryptocurrency is often referred to as a "coin" or "token." In general, most cryptocurrencies are considered fungible assets. For example, Bitcoin is considered fungible because each unit of Bitcoin is equivalent to any other unit, meaning they have the same quality and functionality. Regardless of when a unit of Bitcoin was issued ("mined"), all Bitcoin units are part of the same blockchain and have the same functionality. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Users of cryptocurrency use public and private keys to transfer cryptocurrency from one person or place to another. A public key is typically a set of numbers and/or letters that a cryptocurrency user shares with other users to engage in a transaction in cryptocurrency, whereas a private key is typically a set of numbers and/or letters that the user of an account maintains privately to access his or her cryptocurrency. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. As such, most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and

historical record of every transaction.[1] Although many cryptocurrencies are or purport to be pseudonymous, often law enforcement and currency exchangers can use the blockchain to analyze transactions in cryptocurrency, identify individuals who are using cryptocurrency platforms for illicit purposes, and trace fraud proceeds from victims to one or more exchanges or wallets.

12. *Wallets*: Cryptocurrency is often stored in a virtual account called a wallet, which can exist in, among other forms, an external computer device, a computer, on an application, or online. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. Access to a wallet and the cryptocurrency therein is typically protected by a password only known to the owner or user of the wallet. Wallets can be either "custodial" or "non-custodial" (also referred to as "centralized" or "decentralized"). In the case of a non-custodial wallet, the owner of the wallet has sole control of the wallet's private keys, which enable access to the wallet and any funds contained therein. With a custodial wallet, another party controls the private keys to the wallet. This is usually a cryptocurrency exchange, and the relationship between the exchange and the customer can be considered analogous to the relationship between a traditional bank and its customers, where the bank securely maintains funds deposited by a bank customer.

13. *Exchanges/Exchangers*: Virtual currency "exchangers" and "exchanges", such as Binance, Coinbase, Kraken, and Crypto.com, are individuals or companies that exchange virtual currency for other currencies, including U.S. dollars. Exchanges facilitate the purchase, sale, and transfer of a variety of digital currencies. Exchanges can identify accounts using a variety of target

[1] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

identifiers, including the identifiers provided herein for the SUBJECT ACCOUNTS at the Binance exchange.

14. *Centralized/Decentralized Exchanges*: Centralized exchanges generally maintain a custodial role for the wallets of its customers, and function as trusted intermediaries in cryptocurrency transactions. Decentralized exchanges consist of peer-to-peer marketplaces where users can trade cryptocurrencies in a non-custodial manner, without the need for an intermediary to facilitate the transfer and custody of funds. Decentralized exchanges are often used to trade, or "swap", one type of cryptocurrency for another, for which the user pays a transaction fee. Centralized exchanges that conduct business in the United States are required to verify their customers' identities and abide by Know-Your-Customer/Anti-Money Laundering (KYC/AML) regulations. Currently, decentralized exchanges are generally not required to abide by KYC/AML regulations, as they do not take custody of funds and are merely providing a platform to facilitate trades between individual users.

15. *Chain-hopping*: Chain-hopping is a technique used to conceal the original source of cryptocurrency and to make it more difficult for law enforcement to trace the movement of cryptocurrency. It consists of converting one form of cryptocurrency for another, often multiple times in close succession, or moving cryptocurrency from one blockchain to another, as some types of cryptocurrency can be traded on multiple blockchains. Chain-hopping is a primary technique in the laundering of stolen cryptocurrency or cryptocurrency obtained from illegal activity. Decentralized exchanges are often used in chain-hopping, as they allow one type of cryptocurrency to be converted to another while requiring the user to provide minimal or no identifying information.

16. *Stablecoin*: Stablecoins are a type of cryptocurrency that has price coordinated to a specific reference asset. The reference asset may be fiat money, another cryptocurrency, commodities, or other assets. Common examples of stablecoins are Tether (USDT), USD Coin (USDC), DAI, and Binance USD (BUSD). Each of these stablecoins are pegged to the U.S. dollar and are designed to maintain the value of $1 USD per coin.

FACTS SUPPORTING PROBABLE CAUSE

THE SCHEME

17. The USSS is investigating an investment fraud scam, commonly referred to as "Pig Butchering," perpetrated on victims throughout the United States, including in the Middle District of North Carolina. According to the Global Anti-Scam Organization, [2] a nonprofit aiming to raise awareness and provide tools to combat cybercrime, Pig Butchering originated in China in 2019. The scheme often begins when a scammer sends a victim a seemingly innocuous and misdialed text message, or through sending an unsolicited message to a victim's social media account. From there, the scammer will attempt to establish a more personal relationship with the victim by using manipulative tactics similar to those used in online romance scams.

18. The victims in Pig Butchering schemes are referred to as "pigs" by the scammers because the scammers will use elaborate storylines to "fatten up" victims into believing they are in a romantic or otherwise close personal relationship. Once the victim places enough trust in the scammer, the scammer brings the victim into a cryptocurrency investment scheme. The investment schemes have the appearance of a legitimate enterprise through the use of fabricated interfaces, derivative websites that appear related to legitimate companies, and other techniques designed to bolster the scheme's legitimacy. This generally includes a fake investment platform operated

[2] https://www.globalantiscam.org/

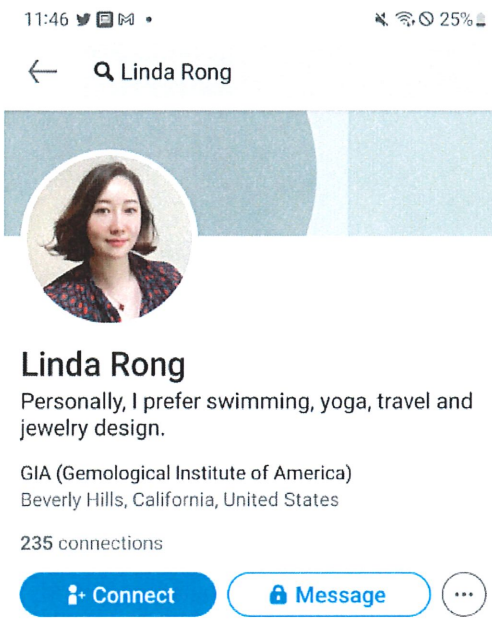
through a website or mobile application that displays a fictitious investment portfolio with abnormally large investment returns.

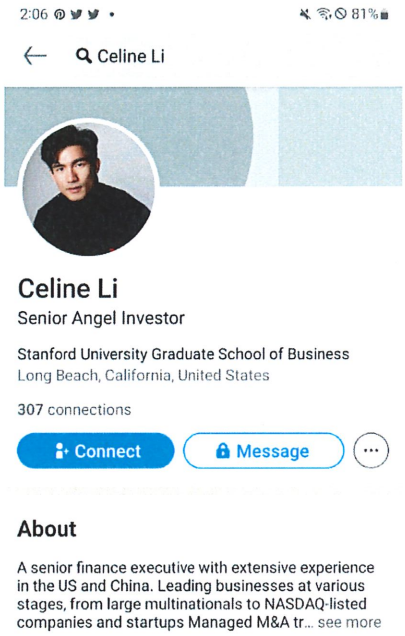
19. The investment platforms are a ruse, and the funds contributed are routed directly to a cryptocurrency address the scammers control. When the victims do attempt to withdraw their funds, they are unable to do so and are often met with various excuses or even required to pay "taxes" in order to release their funds. The "tax" payments are an attempt by the scammers to elicit even more money out of the victims. Eventually, most victims are completely locked out of their accounts and lose all of their funds.

20. In this case, the USSS has identified an organized criminal group which conducts Pig Butchering fraud schemes against victims located across the United States. USSS has attributed fraud cases to this group based on, among other things, victim recruitment tactics, common website domain registration information, fraudulent exchange website appearance and functionality similarity, and shared cryptocurrency addresses and patterns of activity.

a. *Victim recruitment tactics*: Victims are contacted on social media websites, with LinkedIn being the most common. The scammers initiate a conversation and attempt to maintain a continuing relationship with the victim. Once the conversation has started, the scammer will request that the conversation move to the WhatsApp encrypted chat application. The scammer will continue the conversation on WhatsApp, and at some point, will begin talking about their successful cryptocurrency investments. This will generally include a claim that they or a friend/relative have insider knowledge or a trading algorithm which allows them to quickly make large profits on their investments. The scammer will then attempt to recruit the victim into investing in cryptocurrency using a specific

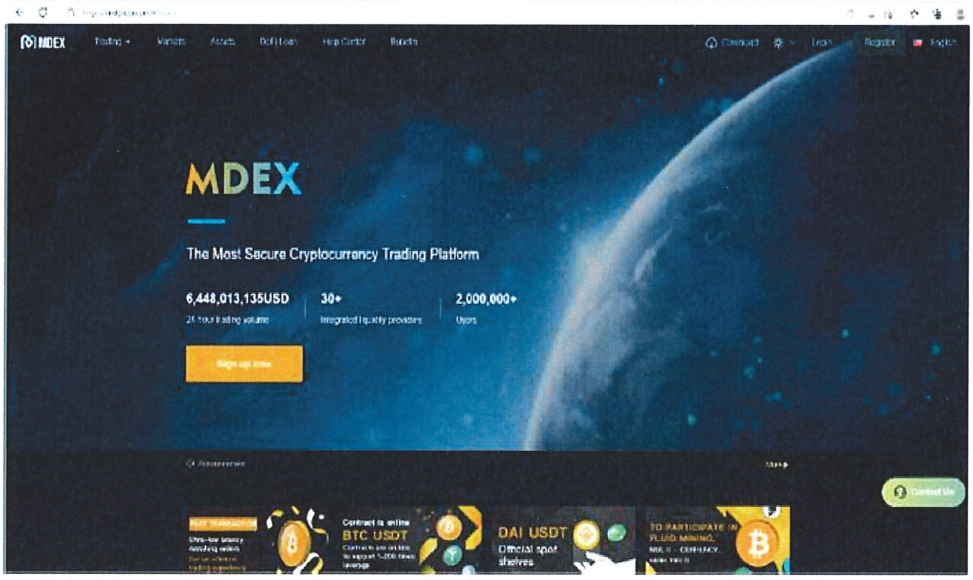
exchange. Below are examples of LinkedIn profiles used to contact and recruit victims by this group of scammers:

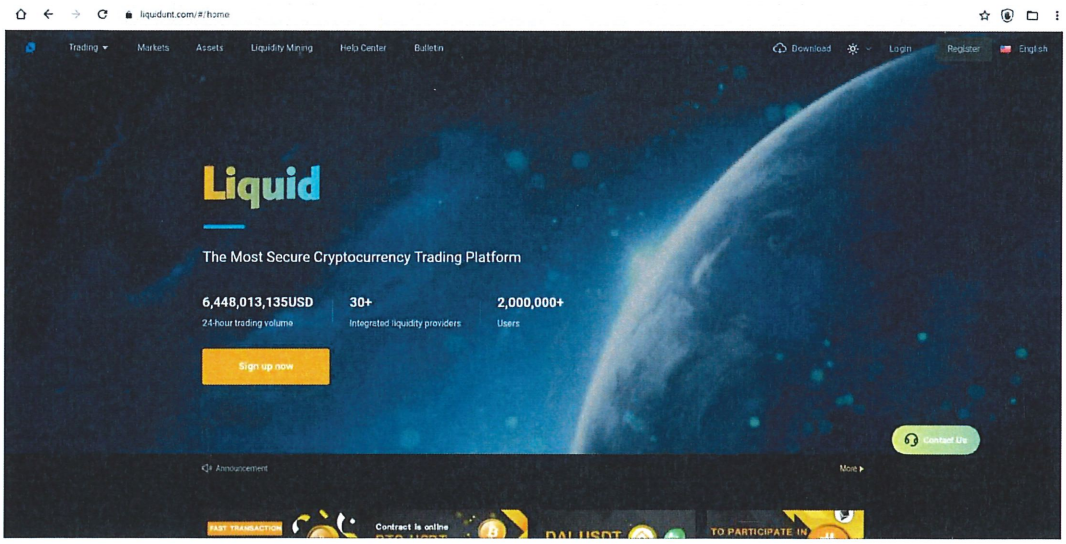




b. *Common website domain registration information*: Through analysis of Internet domain name registration information, this investigation has identified 874 website domains that are linked by common registration information (e-mail address, phone number, and/or address). The "domain" is the website address which is registered and owned by a specific party, which allows them to make content on that domain accessible on the public Internet. The website address is also referred to as a Uniform Resource Locator (URL). All of the identified victims have used one of these 874 domains in order to access what they believed was their cryptocurrency investment account. Many of the domain names are variations on legitimate exchange websites. For example, the victim in this case used the URL "liquidunt.com" to access his account. This is a variation on "liquid.com", which is the URL for the legitimate cryptocurrency exchange Liquid.

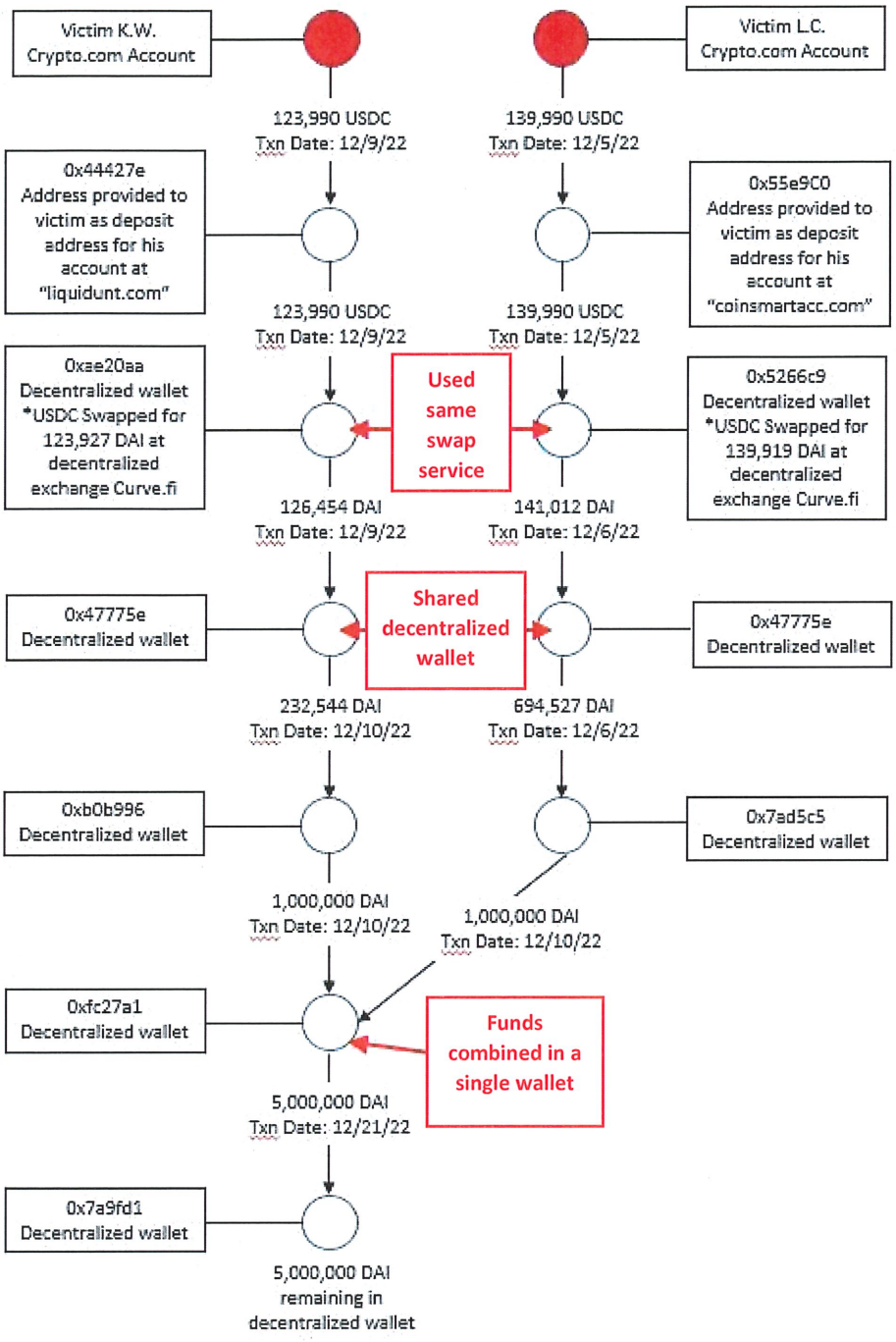
c. *Fraudulent exchange website appearance and functionality*: The fraudulent exchange websites in this scheme share a similar appearance and functionality. Many are identical, with the only change being the name of the site. This suggests that the various exchange websites are under the control of a single group and are using a template to quickly deploy new exchange sites when one is shut down or identified as fraudulent.





d. *Shared cryptocurrency addresses and patterns of activity*: The investigation has identified two cryptocurrency wallet addresses which have been used to launder the

fraud proceeds from two different victims. The movement of the proceeds follow a similar pattern, suggesting that the wallets are being used primarily for fraud and money laundering. Once funds are sent by the victim to the address provided by the fraudulent exchange, the funds are rapidly moved through multiple wallets. During these transactions they are often comingled with additional cryptocurrency, split into smaller amounts, and sent to multiple wallets. During these transactions the funds are "swapped" for a different type of cryptocurrency, and then moved through additional wallets. This technique is also known as "chain-hopping." The swapping of the initial type of cryptocurrency sent by the victim for a different type was observed at least once in the trace of every payment by these victims, and often multiple swaps were observed. As each of these swaps incurs a fee, there is no legitimate purpose to conduct multiple swaps over a short time period, especially when both types of cryptocurrency being swapped are stablecoins pegged to the U.S. dollar, and are therefore valued at an equal amount. The following is an example of the shared wallet activity summarized above. It shows transactions and subsequent tracing of money fraudulently gained from the two different victims. The victims, K.W. and L.C., are believed to be victims of the same fraud group due to the factors described above. K.W. is the Chapel Hill victim whose case is described in detail below. The victims were discovered independently, they were contacted and recruited by different people on LinkedIn, and they used different fraudulent exchange websites to deposit cryptocurrency in their accounts. For clarity, all cryptocurrency addresses have been shortened to the first eight characters.



In my training and experience, all of these tactics (moving funds rapidly between wallets, splitting funds between multiple wallets, and swapping/chain-hopping) are used by organized criminal groups in order to obscure the source of cryptocurrency and make it more difficult to be traced on the blockchain. Based on my review of K.W.'s transactions

and other transactions associated with those wallets, I believe that from November 1, 2022 to January 20, 2023, the funds of approximately 73 other suspected victims passed through the same decentralized wallet that K.W.'s funds were sent to each time he made a "deposit" to his account on "liquidunt.com". The wallet address that K.W. was given for his deposits, 0x44427e, appears to be a "burner" address, in that it was only used for his deposits and not for any other victims. Each time K.W. made a deposit to this address, it was immediately (within an hour or less) sent to a second decentralized wallet, 0xae20aa. This wallet appears to be a consolidation wallet for the funds of multiple victims, as all of the incoming transactions come from other suspected "burner" wallets where the transaction activity is very similar to K.W.'s initial deposit address. Specifically, the "burner" wallets receive funds from legitimate cryptocurrency exchanges, as in K.W.'s case where he sent funds from his Crypto.com account, and those funds are subsequently sent to the consolidation wallet. I searched the 73 wallet addresses on the Internet Crime Complaint Center (IC3), a U.S. government website for reporting fraud, and found that three of the addresses were associated with fraud reports and described a scheme consistent with the one described above. By analyzing this activity, I found 73 of these suspected "burner" wallets which were sending funds to 0xae20aa. While in the consolidation wallet, the funds are swapped for a different form of cryptocurrency, and then sent out to other decentralized wallets. This activity is described in further detail below.

21. The USSS has identified over 100 likely victims of this specific group through reports submitted by victims on IC3. Seventeen of these victims have been interviewed and confirmed to be victims of this specific criminal group, based on the commonalities described above in paragraph 20a-20c. Based on the large number of Internet domain names registered by

this group, it is highly likely that there are numerous additional victims who have not yet been identified, as each of these domain names appears to represent a fraudulent exchange website which has already been deployed against victims or is available to deploy in the future

Victim K.W.

22. On or about November 12, 2022, within the Middle District of North Carolina and elsewhere, a suspect identified by the name "Linda Rong" committed wire fraud on a victim identified herein as "K.W." K.W. is a seventy-year old resident of Chapel Hill, North Carolina. In or around November 2022, without prompting from K.W., a person claiming to be a woman named Linda Rong contacted K.W. on the LinkedIn professional networking website/application. They began a conversation, which Rong suggested they move to the chat application WhatsApp. Rong began talking to K.W. about her cryptocurrency investments, advised K.W. how he could make a large profit by investing in a cryptocurrency exchange called "Liquid", and provided him with the URL "liquidunt.com". Of note, there is a legitimate cryptocurrency exchange called "Liquid", which is based in Japan and uses the URL "liquid.com". Based on my experience with similar fraud schemes, I believe that the suspects in this case used the name Liquid in order to appear legitimate, while actually being a fraudulent exchange that only existed to further this investment fraud scheme.

23. Rong instructed K.W. to open an account on the legitimate cryptocurrency exchange Crypto.com and on the fraudulent Liquid exchange. Rong further instructed K.W. to purchase USD Coin (USDC) cryptocurrency on Crypto.com and then to send the USDC to a cryptocurrency wallet address supposedly associated with Liquid, which K.W. did using the Crypto.com website and the fraudulent Liquid exchange website (liquidunt.com). Rong provided K.W. with instructions on when to "trade" on Liquid, which would provide him a high rate of

return on his investment. She informed K.W. that he would be able to withdraw funds from Liquid and transfer them back to Crypto.com, where he would be able to sell the USDC for U.S. dollars. K.W. followed this process and conducted his first transaction, using the process outlined above, to transfer 4,990 USDC to the fraudulent Liquid exchange on November 12, 2022.

24. At Rong's urging, K.W. continued to invest larger amounts, using the same process to transfer a total of approximately 826,440.51 USDC from November 12, 2022 to December 14, 2022. This total includes K.W.'s initial "investments", as well as "taxes" and a "user authentication fee", which the fraudulent Liquid exchange's customer service informed him he was required to pay in order to withdraw any of his funds. K.W. was informed that he could not pay these taxes and fees from the account balance, and had to pay them separately by sending USDC to the same cryptocurrency address as his initial investment. After paying the required taxes and fees, K.W. was still not able to withdraw any funds from his account. At that point he was asked for further fees in order to conduct a withdrawal, which he did not pay. All payments made by K.W. were sent to 0x44427e, a decentralized wallet which K.W. believed was the deposit address for his Liquid account based on information he was provided on the fraudulent Liquid website.

Tracing of Victim Funds to the SUBJECT ACCOUNTS

25. Two of K.W.'s USDC transfers were traced to accounts at Binance, as detailed below. The traces were conducted using the Last-In-First-Out accounting principle – meaning that the most recently deposited items are recorded as the next withdrawal.

SUBJECT ACCOUNT #1:

26. On December 1, 2022, K.W. transferred 69,900 USDC from his Crypto.com wallet to the address provided by the fraudulent Liquid exchange. From December 1 to December 23, 2022, the funds were moved between several decentralized wallets, as detailed below, while being

comingled with additional cryptocurrency and converted to different forms. On December 23, 2022, 69,800 USDT was sent to Binance wallet address 0x9510c00aaac3561ef75f7b111edfcba1278333b6 (SUBJECT ACCOUNT #1). As of January 5, 2023, when law enforcement requested Binance to freeze the account, approximately 402,822.131 USDT was present in SUBJECT ACCOUNT #1. Of this amount, 69,800 USDT can be traced as proceeds directly from the victim. The remaining 333,022.131 USDT was received in the account from other sources.

27. Based on shared wallet activity observed in this case, as explained in paragraph 20(d) above, as well as the transaction volume and pattern of activity for SUBJECT ACCOUNT #1, there is probable cause to believe that the funds in SUBJECT ACCOUNT #1 are involved in money laundering. An analysis of the transaction history for SUBJECT ACCOUNT #1, from March 4, 2022 to January 5, 2023 (when the account appears to have been the most active), shows that approximately 37,121,952 USD-equivalent was deposited in the account over 475 transactions, and approximately 36,884,490 USD-equivalent was withdrawn over 247 transactions. The total amount of deposits and withdrawals from SUBJECT ACCOUNT #1 are roughly equal, indicating that the account holder is not the intended recipient of the funds. Deposits were generally withdrawn within one day, the majority for the same amount as the deposit, or consolidated with other deposits made around the same time and withdrawn together. This pattern is indicative of a "mule" account, used to obscure the source and movement of illegitimate funds by layering them with funds from other sources, both legitimate and illegitimate.. Additional analysis shows that a large percentage of the total deposits and withdrawals for SUBJECT ACCOUNT #1 came from a small subset of addresses: 264 of the 487 deposits (56%) came from 8 addresses, and 166 of the 247 withdrawals (67%) were sent to 8 other

addresses. This pattern is also suggestive of a "mule" account, with repeated transactions to and from the same addresses. The account also demonstrates the use of "chain-hopping", as 47 of the 475 deposits (10%) were made on the Ethereum blockchain, while all 475 withdrawals were made on the TRX blockchain. Finally, Binance records indicate that there were no purchases or withdrawals of any assets in this wallet from a traditional bank account, or any transactions to or from fiat currency (i.e. all deposits and withdrawals were transferred in and out from other cryptocurrency addresses). Based on my training and experience, wallets with high levels of transaction activity, that include no deposits or withdrawals involving fiat currency or traditional bank accounts, and transact primarily in stablecoins like USDT/USDC, are known to be used for money laundering. As there is no connection to a traditional bank or any transaction involving fiat currency, the sole purpose of this account appears to be receiving large amounts of cryptocurrency and quickly sending it elsewhere, with the majority of these transactions involving a limited number of addresses.

28. A summary and graphical representation of the transfers from K.W. to SUBJECT ACCOUNT #1 follows:

a. 12/1/2022: 69,990 USDC was sent from K.W.'s Crypto.com account to 0x44427e (address provided to victim by fraudulent Liquid exchange).

b. 12/1/2022: 69,990 USDC sent from 0x44427e to 0xae20aa (decentralized wallet). The USDC is sent to decentralized exchange Curve.fi and converted to DAI (minus a fee), then sent back to 0xae20aa as 69,953.14 DAI.

c. 12/1/2022: 69,913.14 DAI sent from 0xae20aa to 0x23955b (decentralized wallet). While in this wallet the DAI is comingled with additional funds.

d. 12/2/2022: 733,052.483115 DAI sent from 0x23955b to 0x3942cd (decentralized wallet). The DAI is sent to decentralized exchange Curve.fi and converted to USDT (minus a fee), then sent back to 0x3942cd as 733,052.483115 USDT, where it is comingled with additional USDT.

e. 12/2/2022: 735,126 USDT sent from 0x3942cd to 0x3a3ec8 (decentralized wallet). While in this wallet the USDT is comingled with additional funds.

f. 12/2/2022: 1,500,000 USDT sent from 0x3a3ec8 to 0x71fd4b (decentralized wallet).

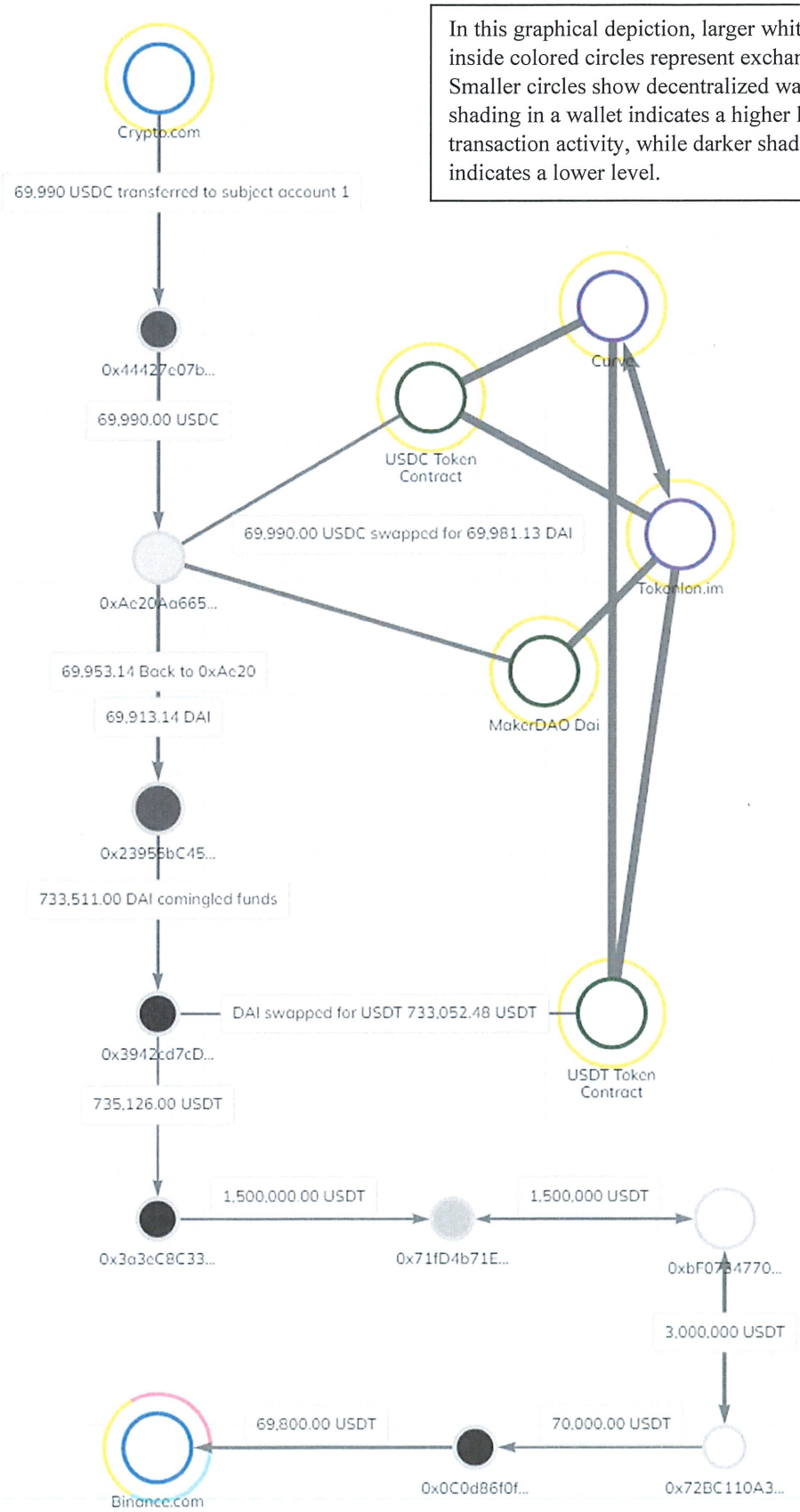
g. 12/3/2022: 1,500,000 USDT sent from 0x71fd4b to 0xbf0734 (decentralized wallet). While in this wallet the USDT is comingled with additional funds.

h. 12/4/2022: 3,000,000 USDT sent from 0xbf0734 to 0x72bc11 (decentralized wallet).

i. 12/23/2022: 70,000 USDT sent from 0x72bc11 to 0x0c0d86 (decentralized wallet).

j. 12/23/2022: 69,800 USDT sent from 0x0c0d86 to 0x9510c0 (SUBJECT ACCOUNT 1 at Binance).

In this graphical depiction, larger white circles inside colored circles represent exchanges. Smaller circles show decentralized wallets; lighter shading in a wallet indicates a higher level of transaction activity, while darker shading indicates a lower level.



SUBJECT ACCOUNT #2:

29. On December 2, 2022, K.W. transferred 49,990 USDC from his Crypto.com wallet to the address provided by the fraudulent Liquid exchange. From December 2 to December 16, 2022, the funds were moved between several decentralized wallets, as detailed below, while being comingled with additional cryptocurrency and converted to different forms. On December 16, 2022, 304,514 USDT was sent to Binance wallet address 0xe4f410. Transaction records for this Binance account show that in the span of four minutes from being deposited, the funds were converted to USDC and then withdrawn as 303,600 USDC to a non-Binance decentralized wallet address. These funds were traced to several additional decentralized wallets, while again being comingled with additional cryptocurrency. On December 26, 2022, approximately 2,000,000 USDC was sent to Binance wallet address 0xf85db42fc79b153eac3725f0382fadaa34bae40a (SUBJECT ACCOUNT #2). As of January 5, 2023, when law enforcement requested Binance to freeze the account, approximately 17,926.991 USDT and 1,250,000.15 BUSD was present in the account (originally deposited as USDC).[3] Of this amount, the 17,926.991 USDT can be traced as proceeds directly from K.W. The 2,000,000 USDC sent to the account was automatically converted to BUSD by Binance, and then converted by the account holder to USDT. The remaining amount was received in the account from other sources.

30. Based on shared wallet activity observed in this case, as detailed in paragraph 20(d) above, as well as the transaction volume and pattern of activity for this account, there is probable cause that the funds in SUBJECT ACCOUNT #2 are involved in money laundering. An analysis of the transaction history for SUBJECT ACCOUNT #2, from July 6, 2022to January 6, 2023

[3] Binance USD (BUSD) is a stablecoin issued by Binance. Binance's policy is to automatically convert USDC deposited into user accounts into BUSD.

(when the account appears to have been the most active), shows that a total of approximately 62,618,632 USD-equivalent was deposited in the account over 65 transactions, and approximately 62,697,509 USD-equivalent was withdrawn over 77 transactions. The total amount of deposits and withdrawals are roughly equal, indicating that the account holder is not the intended recipient of the funds. Deposits were generally withdrawn within one day, the majority for the same amount as the deposit, or consolidated with other deposits made around the same time and withdrawn together. This pattern is indicative of a "mule" account, used to obscure the source and movement of illegitimate funds by layering them with funds from other sources, both legitimate and illegitimate. Additional analysis shows that a large percentage of the total deposits and withdrawals in SUBJECT ACCOUNT #2 came from a small subset of addresses: 52 of the 65 deposits (80%) came from 4 addresses, and 65 of the 77 withdrawals (84%) were sent to 4 other addresses. This pattern is also suggestive of a "mule" account. The account also demonstrates extensive use of "chain-hopping", as 46 of the 65 deposits (70%) were made on the Ethereum blockchain, while 60 of the 77 withdrawals (78%) were made on the TRX blockchain. Finally, Binance records indicate that there were no purchases or withdrawals of any assets in this wallet from a traditional bank account, or any transactions to or from fiat currency (i.e. all deposits and withdrawals were transferred in and out from other cryptocurrency addresses). Based on my training and experience, wallets with high levels of transaction activity, that include no deposits or withdrawals involving fiat currency or traditional bank accounts, and transact primarily in stablecoins like USDT/USDC, are known to be used for money laundering. As there is no connection to a traditional bank or any transaction involving fiat currency, the sole purpose of this account appears to be receiving large amounts of cryptocurrency and quickly sending it elsewhere, with the majority of these transactions involving a limited number of addresses. The fact that deposits in this account are

often converted to different forms of cryptocurrency, and/or withdrawn on different blockchains, is further evidence of attempts to obscure the initial source of the funds, and make it more difficult to trace.

31. A summary and graphical representation of the transfers from K.W. to SUBJECT ACCOUNT 2 follows:

a. 12/2/2022: 49,990 USDC was sent from K.W.'s Crypto.com account to 0x44427e (address provided to victim by fraudulent Liquid exchange).

b. 12/2/2022: 49,990 USDC sent from 0x44427e to 0xae20aa (decentralized wallet). The USDC is sent to decentralized exchange Curve.fi and converted to DAI (minus a fee), then sent back to 0xae20aa as 49,965.66 DAI, where it is comingled with additional DAI.

c. 12/2/2022: 60,960.209 DAI sent from 0xae20aa to 0x23955b (decentralized wallet). While in this wallet the DAI is comingled with additional funds.

d. 12/3/2022: 479,871 DAI sent from 0x23955b to 0x7ad5c5 (decentralized wallet). While in this wallet the DAI is comingled with additional funds.

e. 12/5/2022: 800,855 DAI sent from 0x7ad5c5 to 0x196d33 (decentralized wallet). While in this wallet the DAI is comingled with additional funds.

f. 12/5/2022: 3,000,000 DAI sent from 0x196d33 to 0x81e991 (decentralized wallet).

g. 12/6/2022: 2,000,000 DAI sent from 0x81e991 to 0xa2c75e (decentralized wallet). The DAI is sent to decentralized exchange Curve.fi and converted to USDT (minus a fee), then sent back to 0xa2c75e as 1,999,804.869678 USDT.

h. 12/6/2022: 1,999,805 USDT sent from 0xa2c75e to 0xa55c9b (decentralized wallet).

i. 12/6/2022: 1,820,000 USDT sent from 0xa55c9b to 0x483840 (decentralized wallet).

j. 12/6/2022: 663,097 USDT sent from 0x483840 to 0x0ed4e7 (decentralized wallet).

k. 12/13/2022: 663,097 USDT sent from 0x0ed4e7 to 0xc8abbe (decentralized wallet).

l. 12/14/2022: 300,000 USDT sent from 0xc8abbe to 0xe76591 (decentralized wallet).

m. 12/14/2022: 99,900 USDT sent from 0xe76591 to 0x63902e (decentralized wallet).

n. 12/16/2022: 99,900 USDT sent from 0xe76591 to 0x63902e (decentralized wallet). While in this wallet the USDT is comingled with additional funds.

o. 12/16/2022: 296,990 USDT sent from 0x63902e to 0xbb4f12 (decentralized wallet). While in this wallet the USDT is comingled with additional funds.

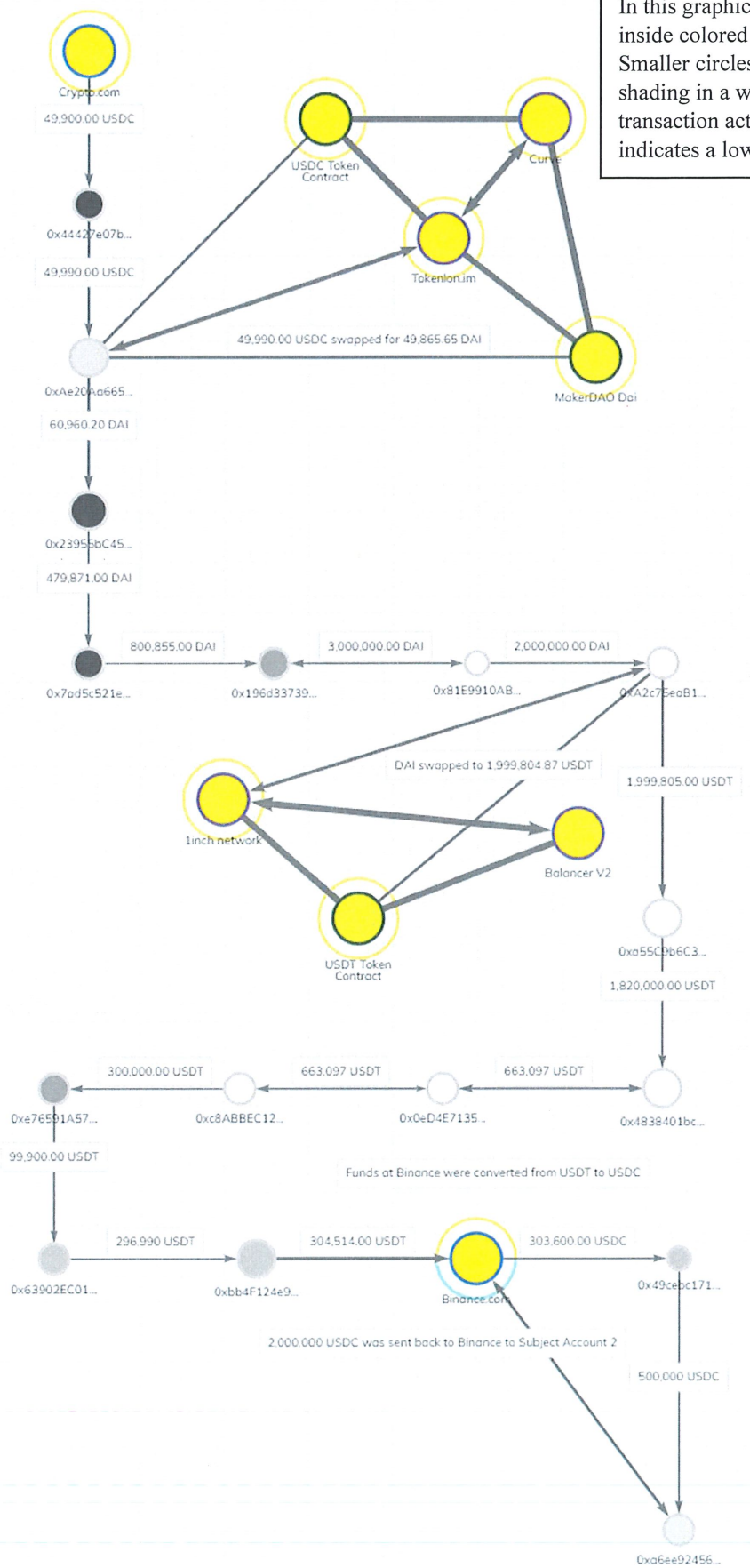
p. 12/16/2022: 304,514 USDT sent from 0xbb4f12 to 0xe4f410 (Binance account address). Based on account records received from Binance, this account belongs to Wai Chung Chong, who appears to be located in Hong Kong based on his account activity log. Transaction records show that in the span of four minutes from being deposited, the USDT was converted to USDC and then withdrawn, as detailed below.

q. 12/16/2022: 303,600 USDC sent from 0xe4f410 to 0x49cebc (decentralized wallet). While in this wallet the USDC is comingled with additional funds.

r. 12/26/2022: 500,000 USDC sent from 0x49cebc to 0xa6ee92 (decentralized wallet). While in this wallet the USDC is comingled with additional funds.

s. 12/26/2022: 2,000,000 USDC sent from 0xa6ee92 to 0xf85db4 (SUBJECT ACCOUNT 2 at Binance).

In this graphical depiction, larger white circles inside colored circles represent exchanges. Smaller circles show decentralized wallets; lighte shading in a wallet indicates a higher level of transaction activity, while darker shading indicates a lower level.



CONCLUSION

32. Based on information derived from the foregoing investigation, there is probable cause to conclude that the SUBJECT ACCOUNTS received the proceeds of a wire fraud and money laundering scheme in violation of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and conspiracy to commit wire fraud), and Title 18, United States Code, Sections 1956(a)(1)(B)(i) and 1956(h) (money laundering and conspiracy to commit money laundering). Those proceeds are subject to seizure and forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c). In addition, there is probable cause to believe that the SUBJECT ACCOUNTS constitute property involved in money laundering transactions in violation of Title 18, United States Code, Section 1956, and are therefore subject to seizure and forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 982(a)(1). Accordingly, I respectfully request that warrants be issued authorizing the seizure of all funds in the SUBJECT ACCOUNTS.

33. I submit that a protective or restraining order issued pursuant to Title 21, United States Code, Section 853(e) would be insufficient to ensure the availability of the funds in the SUBJECT ACCOUNTS for forfeiture. Cryptocurrency can be transferred faster than traditional bank funds, and once transferred, generally cannot be recalled to an original wallet. Moreover, there is a risk that the funds may be moved to a location where no forfeiture or seizure would be possible, at which point the funds could be further laundered into a "privacy" (i.e. untraceable) cryptocurrency. Thus, I submit that a seizure warrant is the only means to reasonably assure the availability of the funds in the SUBJECT ACCOUNTS for forfeiture.

/s/ Steven Robinson
Steven S. Robinson
Special Agent
United States Secret Service

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of this written affidavit.

1/26/2023

JOI ELIZABETH PEAKE
UNITED STATES MAGISTRATE JUDGE